UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,065	11/15/2006	Yingxin Huang	CU-5029 WWP	5957

26530 7590 04/06/2009
LADAS & PARRY LLP
224 SOUTH MICHIGAN AVENUE
SUITE 1600
CHICAGO, IL 60604

EXAMINER	
SHAHEED, KHALID W	
ART UNIT	**PAPER NUMBER**
2617	

MAIL DATE	DELIVERY MODE
04/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/591,065	**Applicant(s)** HUANG ET AL.	
	Examiner KHALID SHAHEED	**Art Unit** 4182	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-15_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-15_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)☒ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _02/07/2007, 08/03/2007, 12/07/2007_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Status

1. Claims 1- 15 are pending.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over 3GPP TS 33.220 v6.0.0 (2004-03) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping architecture (Release 6) 22 March 2004, pages 1-18 (XP002422872) {herein after referred to as 3GPP} in view of Faccin et al. (WO 2003-02-20)

In regards to claim 1, 3GPP discloses a method for a user to establish a security association with an application server, wherein the user has completed a mutual authentication with a Bootstrapping Server Function (BSF) that performs user identity initial verification in a generic authentication architecture in his home network, and obtained a Bootstrapping-Transaction Identifier (B-TID) assigned to him by the BSF (sections4.2.1,4.2.2, 4.3.7, figures 3, 5).

3GPP does not disclose that when the user roams in a visited network, after receiving a service request from the roaming user, the application server in the visited network establishes a security association with the roaming user after getting the user's information from the roaming user's home network. The problem to be solved by the present invention may therefore be regarded as how to establish security associations with the application server when a user is roaming
in a visited network.

Faccin has already disclosed a feature employed for the same purpose wherein an application server in the visited network contacts the roaming user's home network in order to establish a security association, (page 3, line 15-page 4, line 1 ;page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2;claim 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention, namely when the same result is to be achieved (see page 8, lines 27-28 of document 3GPP; page 2, lines 9-23 of document Faccin), to apply these features with corresponding effect to the method to establish security association according to document 3GPP, thereby arriving at a method for a roaming user to establish a security association according to claim 1. The motivation for combing the invention of Faccin with that disclosed by 3GPP would be to efficiently negotiate security associations establishment between a mobile nodes connected to the wireless terminal and different network entities.

In regards to claim 2, 3GPP discloses the step of obtaining a user's user information comprises: the application server in sending a query message to an authentication entity in the local network to inquire the user information associated with the B-TID (“fetch the required authentication information”) (Section 4.4.3); the authentication entity which received the message finding out the home network to which the user belongs according to the B-TID in the message (“detect the home network”; Section 4.3.7), and acquiring the user information associated with the B-TID from the BSF in the roaming user's home network (“user profile”; #2 in Section 4.5.2 & Figure 3), and returning the acquired the user information to the application server (direction of arrow towards BSF, Fig. 3); the application server in the visited network obtaining the user information according to a response message returned from the authentication entity (#4 & #5 in Fig. 3).

3GPP does not disclose that a roaming users' information is obtained while in a visiting network or that the application server is in a visiting network.

Faccin discloses that a roaming user's information is obtained while in a visited network (Fig. 2) and that the application server is in a visiting network querying information form the home/local network(page 3, line 15-page 4, line 1 ;page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; claim 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention, to include that feature of locating and obtaining subscriber information utilizing an application server in a visited network as disclosed by Faccin within the technical disclosure document of 3GPP. The motivation for doing so would be allow allowed a network to protect itself from user fraud.

In regards to claim 3, 3GPP discloses the method wherein the authentication entity is a BSF (Fig. 1) or a generic authentication architecture proxy; the step of the BSF or the generic authentication architecture proxy in the network acquiring the user information associated with the B-TID from the user's home network comprises (Section 4.3.7) and inquiring about the user information associated with the B-TID (Section 4.4.3); and obtaining the user information associated with the B-TID from the response message returned by the BSF in the roaming user's home network (Section 4.3.7).

3GPP does not explicitly disclose an example where the BSF or the generic authentication architecture proxy in the visited network directly sending a query message to the BSF in the roaming user's home network,

Faccin discloses a security connection between two generic authentication (AAA) servers wherein one server is located in home network and the other in visited network wherein an application server in the visited network contacts the roaming user's home network in order to establish a security association, (page 3, line 15-page 4, line 1 ;page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2;claim 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention, namely when the same result is to be achieved (see page 8, lines 27-28 of document 3GPP; page 2, lines 9-23 of document Faccin), to apply these features with corresponding effect to the method to establish security association according to document 3GPP, thereby arriving at a method for a roaming user to establish a security association according to claim 1. The motivation for doing so would be allow certain users to watch mobile video programming while traveling in a automobile, train or some other moving apparatus.

In regards to claim 4, 3GPP discloses a completed mechanism for operating a bootstrapping function with a network. 3GPP further identifies a Generic Authentication Architecture (Section 4.3.5)

3GPP does not further disclose a method wherein the generic authentication architecture proxy in the visited network is an independent server, or a server combined with an AAA server in the local network, or a server combined with the application server in the local network.

Faccin clearly discloses a method wherein the generic authentication architecture proxy in the visited network is a independent server or a AAA server in the local network combined with the application server in the local network (page 3, line 15-page 4, line 1; page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2; claim 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention for the 3GPP to logically include a generic authentication architecture based on the use of independent server types or with an AAA server as disclose by Faccin. The motivation would be to secure personal user information within a mobile network.

In regards to Claim 5, 3GPP discloses a completed mechanism for operating a bootstrapping function with a network. 3GPP further identifies a Generic Authentication Architecture wherein the Home network sends the subscribers GAA profile information needed for security purposes to the BSF (Section 4.3.5). Presumably the Home network would send the GAA profile information as needed to a BSF that queries the information associated with the B-TID (Section 4.4.3) it in a visiting network.

However 3GPP does not explicitly disclose an AAA server in the home network. Additionally 3GPP does not disclose an AAA server in the visited network.

Faccin discloses a AAA server in the home network inquiring the a Subscriber Database in the in the local network (Fig. 2-4), after the Database in the local network finding the user information associated with the ("identifying information", Abstract), it returning a response message, with the user information associated with the (identifying information) in it, to the local AAA server, and the AAA server returning a response message, with the user information associated with the (identifying information) in it, to the AAA server in the visited network; the AAA server in the visited network obtaining the user information associated with the (identifying information) from the response message returned by the AAA server in the roaming user's home network (page 3, line 15-page 4, line 1 ;page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2;claim 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention, namely when the same result is to be achieved (see page 8, lines 27-28 of document 3GPP; page 2, lines 9-23 of document Faccin), to apply the features disclosed by Faccin as they relate to identifying information/B-TID with corresponding effect to the method to establish security association according to document 3GPP, thereby arriving at a method for a roaming user to establish a security association according to claim 1. The motivation for doing so would be allow mobile operators to operate/provide multiple secured networks multiple different organizations at once.

In regards to claim 6, 3GPP discloses the method wherein, the step of obtaining the roaming user's user information comprises:

Notification user that the B-TID is an illegal identity ("unauthorized"; Section 4.5.2, Fig. 3, Section A.2 & Fig. a1), and indicating the user to use a permanent identity (integrity key/ck; Section 4.5.2);

having received the service request message from the user again, with the permanent identity (Integrity Key) carried in the message,

the BSF in the home network carrying out mutual authentication with the user via the (un-described GAA Mechanism; Section 4.3.5), the BSF in the home network directly returning a successful authentication message carrying the user information to the AAA server (un-described GAA Mechanism; Section 4.3.5) in the local network (Section 4.5.2 in Figure 3),

3GPP does not specifically disclose a user roaming in a visited network nor does 3GPP disclose the exact specifications of the Generic Authentication Architecture disclose in (Section 4.3.5). Therefore 3GPP does not explicitly site the use of AAA server mechanisms in authenticating users after the application server in the visited network obtains a users information (Section 4.4.3).

However Faccin discloses the application server (Agent, Fig. 3) in the visited network notifying the roaming user with a integrity key/Long term ki (Fig. 3 & Page 9, lines 11-20) for identity determination (Fig. 3).The application server in the visited network sending an authentication request to a AAA server in the local network;

the AAA server in the visited network finding out the user's home network according to the user's permanent identity, and sending another authentication request to the AAA server in the roaming user's home network (page 3, line 15-page 4, line 1; page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2; claim 4).

Having received the authentication request from the AAA server in the visited network, the AAA server in the home network sending a request to the BSF in the local network for authentication of the user (page 3, line 15-page 4, line 1; page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2; claim 4);

The application server in the visited network sending an authentication request to a AAA server in the local network ("Home Network", Fig. 2); the AAA server in the visited network finding out the user's home network according to the user's permanent identity ("integrity key/long term ki"; Fig. 3 & Page 9, lines 11-20), and sending another authentication request (CK(RAND2); Fig. 3) to the AAA server in the roaming user's home network (page 3, line 15-page 4, line 1 ;page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2;claim 4);

The application server (Agent) in the visited network obtaining the roaming user's user information from the successful authentication message (Final Results; Fig 3 & 4) returned by the AAA server in the local network (page 3, line 15-page 4, line 1; page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2; claim 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention, namely when the same result is to be achieved (see page 8, lines 27-28 of document 3GPP; page 2, lines 9-23 of document Faccin), to include a authentication mechanism including AAA servers in a visiting network to interface with the BSF disclosed by 3GPP in the Home network with corresponding effect to establish security association according to document 3GPP, thereby arriving at a method for a roaming user to establish a security association according to claim 1. The motivation for combing the invention of Faccin with the technical disclosure 3GPP would be to efficiently negotiate security associations establishment between a mobile nodes through the use of AAA servers as is a industry standard to insure efficient security handshake negotiation.

In regards to claim 7, 3GPP discloses wherein the user information comprises at least: key information and the user's identity (“bind the subscriber identity to the keying material”; Section 4.3.7).

In regards to claim 8, 3GPP discloses wherein the user information also comprises the profile information associated with security (“profile information needed for security purposes”; Section 4.3.5).

In regards to claim 9, 3GPP disclose the method wherein the key information is a shared key Ks generated (shared key material) in authentication, or a Ks-derived key and its valid term (Section 4.2.2, Section 4.3 & Section 4.5.2).

In regards to claim 10 & 11; 3GPP discloses the method wherein the user information comprises at least: key information and the user's identity (“bind the subscriber identity to the keying material”; Section 4.3.7).

In regards to claim 12 & 13; 3GPP discloses the method wherein the user information also comprises the profile information associated with security (“profile information needed for security purposes”; Section 4.3.5).

In regards to claim 14 & 15; 3GPP discloses the method wherein the key information is a shared key Ks generated in authentication, or a Ks-derived key and its valid term (Section 4.2.2, Section 4.3 & Section 4.5.2).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Haukka et al. (US 2005/0102501 A1) discloses a shared secret usage for bootstrapping.

Faccin et al. (US 7,213,144 B2) discloses an efficient security association establishment negotiation technique.

Faccin et al. (US 6,879,690) discloses a method and system for delegation of security procedures to a visited domain.

Buddhikot et al. (US 7, 231, 521) discloses a scheme for authentication and dynamic key exchange.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to KHALID SHAHEED whose telephone number is (571)270-5813. The examiner can normally be reached on Monday-Friday 8am-5pm; EST; ALT Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, V. Paul Harper can be reached on 571-272-7605. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VINCENT P. HARPER/

Supervisory Patent Examiner, Art Unit 2617

ks